DİJİTAL DÖNÜŞÜM VE SİBER GÜVENLİK DERNEĞİ

DEĞERLENDİRME YAZISI

www.ddsgd.org

Yapay Zekâ Çağında Siber Güvenlik: MİA Raporu Işığında Türkiye İçin Fırsatlar ve Riskler

Milli İstihbarat Akademisi'nin Stratejik Raporu, Dijital Güvenliği Ulusal Bir Öncelik Olarak Yeniden Tanımlıyor

Yapay zekâ, çağımızın en dönüştürücü teknolojisi olarak hem büyük fırsatlar hem de öngörülmesi güç riskler sunuyor. Milli İstihbarat Akademisi (MİA) tarafından Nisan 2026'da yayımlanan ve bu günlerde yeniden gündemin merkezine oturan "Yapay Zekâ Çağında Siber Güvenlik ve Türkiye'nin Stratejik Öncelikleri" başlıklı rapor, bu ikili tabloyu stratejik bir çerçevede ele alması bakımından son derece kıymetli bir belge niteliğinde.

Dijital Dönüşüm ve Siber Güvenlik Derneği olarak, bu raporu yalnızca bir tehdit analizi değil; aynı zamanda Türkiye'nin dijital olgunluğunu artırma yolunda bir yol haritası olarak okuyoruz. Bu değerlendirmede, raporun ortaya koyduğu fırsatları ve riskleri dengeli bir bakışla ele alıyoruz.

Paradigma Değişimi: Siber Güvenlik Artık Sadece Teknik Bir Mesele Değil

Raporun en önemli tespiti, siber güvenliğin artık yalnızca cihazların, uygulamaların ve veri tabanlarının korunmasıyla sınırlı bir teknik alan olmaktan çıktığıdır. **Rapor, yapay zekâyı; saldırı ölçeğini, savunma hızını, karar süreçlerini, tedarik zincirlerini ve düzenleyici ihtiyaçları aynı anda dönüştüren stratejik bir "güç çarpanı" olarak değerlendiriyor.**

Bu yaklaşım, siber güvenliği; veri güvenliği, kurumsal süreklilik, kamu hizmetlerinin kesintisiz yürütülmesi, toplumsal güvenin korunması ve ulusal kapasitenin güçlendirilmesi gibi başlıklarla birlikte ele alınması gereken çok boyutlu bir mesele olarak konumlandırıyor. Derneğimizin de savunduğu bu bütüncül bakış açısı, artık resmî bir strateji belgesinde de karşılık buluyor.

Yeni Nesil Riskler: Büyük Dil Modellerinin Getirdiği Zorluklar

Rapor, yapay zekânın yarattığı yeni ve kendine özgü risk alanlarını da açık biçimde ortaya koyuyor. Özellikle büyük dil modeli (LLM) tabanlı sistemlerin ürettiği tehditler dikkat çekici:

- **İstem enjeksiyonu (prompt injection):** Modellerin kötü niyetli girdilerle yönlendirilmesi
- **Güvensiz çıktı işleme:** Model çıktılarının denetimsiz kullanılmasından doğan açıklar
- **Hassas bilgi sızıntısı:** Gizli verilerin model üzerinden dışarı sızması
- **Tedarik zinciri zafiyetleri:** Dış kaynaklı model ve bileşenlerden gelen riskler
- **Aşırı yetki ve aşırı güven:** Sistemlere gereğinden fazla karar yetkisi tanınması

Raporun kritik bir uyarısı da şudur: Bu riskler yalnızca teknik zaaflar olarak görülmemeli; **veri yönetişimi, denetim, hesap verebilirlik ve kurumsal karar kalitesi** sorunları olarak da değerlendirilmelidir. Ayrıca kimlik manipülasyonu, derin sahte (deepfake) ve sentetik medya gibi tehditler, toplumsal güven açısından ciddi riskler taşıyor.

Madalyonun Diğer Yüzü: Türkiye İçin Stratejik Fırsatlar

Rapor, riskleri ortaya koyarken aynı zamanda güçlü bir fırsat çerçevesi de sunuyor. Öngörülen tehditlere karşı önerilen tedbirler, aslında Türkiye'nin dijital ekosistemini güçlendirecek yatırım alanlarına işaret ediyor. Raporda öne çıkan stratejik öneriler şunlar:

- Test, doğrulama, sertifikasyon ve denetim kapasitesinin geliştirilmesi
- Uzman insan kaynağını güçlendiren sürdürülebilir iş birliği mekanizmalarının kurulması
- Yerli siber güvenlik ve yapay zekâ ekosisteminin desteklenmesi
- Dış teknoloji bağımlılığının güvenlik sonuçlarını yönetebilen güçlü bir ulusal kapasite oluşturulması

Bu öneriler, derneğimizin faaliyet alanıyla birebir örtüşüyor. Nitelikli insan kaynağının yetiştirilmesi, yerli çözümlerin desteklenmesi ve denetim kültürünün kurumsallaşması; hem güvenlik açığını kapatan hem de ekonomik değer üreten bir dönüşümün kapısını aralıyor. Doğru yönetildiğinde, bugünün riskleri yarının en güçlü sektörel fırsatlarına dönüşebilir.

Anahtar Kavram: Yönetişim ve Kalıcı Bir Ulusal Yapı

Raporun belki de en önemli mesajı, yapay zekânın **güvenli, denetlenebilir, hesap verebilir ve dayanıklı bir yönetişim çerçevesi** içinde yönetilmesi gerektiğidir. MİA Başkanı Prof. Dr. Talha Köse'nin de vurguladığı üzere, temel ihtiyaç yalnızca teknolojik gelişmelere uyum sağlamak değil; bu gelişmelerin doğurabileceği riskleri önceden görmek ve gerekli kurumsal tedbirleri zamanında almaktır.

Bu noktada, kimlik manipülasyonu, derin sahte ve sentetik medya risklerine karşı toplumsal farkındalığın artırılması da kritik önem taşıyor. Teknik tedbirler kadar, bilinçli bir toplum ve kurumsal kültür de bu çerçevenin ayrılmaz parçalarıdır.

Sonuç: Riskleri Yöneterek Fırsatları Değerlendirmek

MİA'nın raporu, yapay zekâ çağında siber güvenliğin; devlet kapasitesini, kurumsal karar kalitesini, toplumsal güveni ve stratejik özerkliği birlikte yönetme meselesi olduğunu net biçimde ortaya koyuyor. Türkiye açısından başarının ölçütü ise, yapay zekânın güvenli ve dayanıklı bir ulusal çerçeve içinde yönetilebilmesidir.

Dijital Dönüşüm ve Siber Güvenlik Derneği olarak değerlendirmemiz nettir: Bu rapor, ne salt bir tehdit alarmı ne de gerçekçilikten uzak bir iyimserliktir. Aksine, fırsat ve riski aynı çerçevede ele alan olgun bir stratejik bakışın ürünüdür. Bize düşen görev; farkındalığı artırmak, nitelikli insan kaynağının gelişimine katkı sunmak ve kamu, özel sektör ile akademi arasında sağlam iş birlikleri kurmaktır. Türkiye'nin dijital geleceğini, riskleri sağduyuyla yöneterek ve fırsatları kararlılıkla değerlendirerek, hep birlikte güvenle inşa edeceğiz.

Yararlanılan Kaynaklar

Anadolu Ajansı (AA) – "Milli İstihbarat Akademisi 'Yapay Zeka Çağında Siber Güvenlik' raporu yayımlandı"

TRT Haber – "Milli İstihbarat Akademisi'nden 'Yapay Zeka Çağında Siber Güvenlik' raporu"

Habertürk – "Milli İstihbarat Akademisi raporu: Yapay zeka siber saldırıların etkisini artırıyor"

Haberler.com – "Milli İstihbarat Akademisi 'Yapay Zeka Çağında Siber Güvenlik' raporu"

SDE (Stratejik Düşünce Enstitüsü) – "MİT Yapay Zeka Çağında Siber Güvenlik ve Türkiye'nin Stratejik Öncelikleri Raporu'nu Yayınladı"

Hukuk Dergisi – "Yapay Zekâ Çağında Siber Güvenlik ve Türkiye'nin Stratejik Öncelikleri"

Not: Raporun tam metnine Milli İstihbarat Akademisi'nin resmî kaynaklarından ulaşılabilir.

Taner Çıtak

Dijital Dönüşüm ve Siber Güvenlik Derneği Başkanı

www.ddsgd.org

Bu değerlendirme yazısı, Milli İstihbarat Akademisi tarafından yayımlanan "Yapay Zekâ Çağında Siber Güvenlik ve Türkiye'nin Stratejik Öncelikleri" raporuna ilişkin kamuya açık basın haberleri ve resmî açıklamalar temel alınarak hazırlanmıştır.